CHAPTER

7

NETWORK PROTOCOLS

After reading this chapter and completing the exercises, you will be able to:

- Understand the network protocols supported by Windows 2000
- Configure TCP/IP

In this chapter, we discuss the networking protocols that Windows 2000 supports, as well as how and when to use them. We also discuss the importance of TCP/IP (Transmission Control Protocol/Internet Protocol) and what is required to configure Windows 2000 to employ this protocol for network communications.

Windows 2000 Network Components

Windows 2000 is designed for networking, and includes all the elements necessary for interacting with a network without requiring any additional software. Windows 2000 networking is powerful and efficient, and relatively easy to configure and use, with graphical user interface and wizards for configuration support.

Windows 2000 Professional and Windows 2000 Server (as well as Windows 2000 Advanced Server and Datacenter Server) can function as a network client or as a network server (or both) and can participate in peer-to-peer, client/server, and terminal/host environments. Windows 2000 also has everything needed to access the Internet, including all the necessary protocols and client capabilities, a powerful Web browser (Internet Explorer), and other Internet tools and utilities.

In Windows 2000, numerous components work together to define its networking capabilities. Each component provides one or more individual network functions and defines an interface through which data moves on its way to and from other system components. This allows Windows 2000 to support multiple protocols easily and transparently; applications need only know how to communicate through a standard application programming interface (API), while the modular organization of the operating system shields them from the complex details that can sometimes be involved.

Networking components can be added to or deleted from a Windows 2000 system without affecting the function of other components, except in those cases where such components are bound to other components. (Binding is discussed later in this chapter.) Adding new components brings new services, communications technologies, and other capabilities into existing networks, and allows additional protocols to join the mix at any time.

Network Protocols

Windows 2000 supports three core network transport protocols. Each of these protocols works best on networks of a particular size, where each such network has its own special performance and access requirements. The major network protocols are NetBEUI, NWLink (IPX/SPX), and TCP/IP. Each of these network transports has specific advantages and drawbacks, as outlined in the sections that follow. The following list sums up the important characteristics of each of the three protocols:

- NetBEUI works best on small networks (10 computers or fewer), single-server, or peer-to-peer networks, where ease of access and use are most important. It is an enhanced version of **NetBIOS (Network Basic Input/Output System)**.
- NWLink works best on networks of medium scope (20 servers or fewer in a single facility). It's also important on networks that include NetWare servers.
- TCP/IP works on a global scale, as demonstrated by its use on the Internet. TCP/IP is a complicated, yet powerful transport that scales well from small networks all the way up to the Internet. It is the most widely used of all networking protocols.

NetBEUI

NetBIOS Enhanced User Interface (NetBEUI) implements the simplest of the three basic Windows 2000 transport protocols. It is also sometimes known as the NetBIOS Frame (NBF) transport protocol. IBM developed NetBEUI in the late 1980s for use with the OS/2 and LAN Manager operating systems.

The developers of NetBEUI did not design the protocol to enable networked PCs to function in a complex networked environment, in which routing support is mandatory. Instead, they built NetBEUI to function best within workgroups ranging in size from 2 to 200 computers. Because of this, NetBEUI is not routable, and unfortunately this limitation restricts NetBEUI to purely local LAN segments that contain either Microsoft or IBM networking clients and servers.

Some networks use bridges to move NetBEUI traffic across multiple LAN segments, but NetBEUI is seldom permitted to transmit across any WAN connections that might otherwise be accessible through network routers. NetBEUI is known as an excessively "chatty" protocol, which makes it unsuitable for WAN use. Microsoft's TCP/IP implementations of NBT (or NetBIOS over TCP/IP) and NetBIOS over IPX, combined with the multiprotocol support offered by Windows 2000, make it possible to use nonbroadcast IP or IPX equivalents to provide usable NetBIOS connectivity across router-managed WAN links that routinely block all broadcast traffic.

NetBEUI Advantages

The two primary advantages of NetBEUI are that it is compact and speedy. Although its chatty characteristics make it unsuitable for WAN use, NetBEUI is by far the fastest of all the **TDI (Transport Driver Interface)** transports in Windows 2000. This makes it ideal on small networks where routing is not required. The most significant features of NetBEUI are:

- It is the fastest of all native Windows 2000 protocols on small networks.
- It supports up to 1023 sessions; earlier implementations supported only 254 sessions.
- It has been optimized to perform well across slow serial links.
- It is easy to install and configure because it relies on NetBIOS naming and delivers automatic addressing.
- It is inherently self-tuning, so no analysis or maintenance of its configuration is necessary.
- It incorporates data integrity checks and retransmission for erroneous or lost packets.
- It incurs the lowest memory overhead of all the major Windows 2000 protocols. For older DOS computers, where RAM space for protocols and drivers is scarce and larger protocols may not fit into available memory, this can make all the difference.

NetBEUI Drawbacks

Unroutability and broadcast overhead make NetBEUI unusable on internetworks or on networks that include WAN as well as LAN links. Because of product specificity, NetBEUI is seldom used except in Microsoft and IBM networks. Possibly because of its insularity, there are few if any diagnostic or troubleshooting utilities for NetBEUI. In short, NetBEUI is not a contender for deployment in large, complex networks. (You can practice installing and removing NetBEUI in Hands-on Project 7-6.)

NWLink

NWLink is the Microsoft implementation of Novell's **Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) protocol** stack. Rather than supporting the native Novell **Open Datalink Interface (ODI)**, NWLink works with the **NDIS (Network Driver Interface Specification)** driver technology that's native to Windows 2000; NDIS defines parameters for loading more than one protocol on a network adapter. NWLink is sufficiently complete to support the most important IPX/SPX APIs, including:

- *Novell Windows Sockets:* Provides the interface support for existing NetWare applications written to comply with IPX/SPX
- *NetBIOS over IPX:* Links the NetBIOS interface with the NWLink transport protocol. This is actually the NWNBLink (NetWare-NetBIOS Link) that allows Microsoft networks to use the NetBIOS interface for NetWare Connectivity or to facilitate Microsoft networking using the routable **IPX** transport protocol.

Although IPX/SPX is the default protocol for NetWare prior to version 5, TCP/IP is the default protocol in version 5.

NWLink Advantages

NWLink offers some powerful capabilities that are conspicuously lacking in NetBEUI, including:

- *SPX II:* SPX II is a new version of **SPX** that has been enhanced to support windowing and can set a maximum frame size.
- *Autodetection of frame types:* NWLink automatically detects which IPX frame type is used on a network during initial startup and broadcast advertisement phases. When multiple frame types appear, Windows 2000 defaults to the industry-standard 802.2 frame type.
- *Direct hosting over IPX:* The ability to host ongoing network sessions using IPX transports. Because it eliminates the overhead associated with NetBIOS, direct hosting over IPX can increase network performance by as much as 20% on client computers. This is especially beneficial for client/server applications.

NWLink Drawbacks

On large networks, IPX may not scale well. IPX lacks a built-in facility for centralized address management like the service that DNS provides for TCP/IP. This omission allows address conflicts to occur—especially when previously isolated networks that employed identical defaults or common addressing schemes attempt to interoperate. Novell established an address registry in 1994 (IPX was introduced in 1983), but it is generally neither used nor acknowledged. The Internet Network Information Center (InterNIC) and its subsequent assigns have managed all public IP addresses since 1982. Like its proprietary cousin, NetBEUI, IPX fails to support a comprehensive collection of network management tools. Finally, IPX imposes a greater memory footprint on DOS machines and runs less efficiently than NetBEUI across slow serial connections.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) represents an all-embracing suite of protocols that cover a wide range of capabilities (more than 100 component protocols that belong to the TCP/IP suite have been standardized).

TCP/IP has also been around for a long time; the original version of TCP/IP emerged from research funded by the Advanced Research Projects Agency (ARPA, a division of the U.S. Department of Defense). Work on this technology began in 1969, continued throughout the 1970s, and became broadly available in 1981 and 1982. Today, TCP/IP is the most common networking protocol in use worldwide, and it is the protocol suite that makes the Internet possible.

TCP/IP has become the platform for a wide variety of network services, including newsgroups (NNTP), electronic mail (SNMP and MIME), file transfer (FTP and ANS), remote printing (lpr, lpd, lpq utilities), remote boot (bootp and **DHCP—Dynamic Host Configuration Protocol**), and the World Wide Web (HTTP—Hypertext Transfer Protocol).

To provide NetBIOS support using TCP/IP transports, Microsoft includes an implementation of NBT (NetBIOS over TCP/IP) with Windows 2000. Microsoft extends the definition of NBT behaviors by adding a new type of NetBIOS network node to the NBT environment, called an "H" node. An H node inverts the normal behavior of the standard NBT "M" (or Mixed) node. It looks first for a NetBIOS name service, such as a **Windows Internet Naming Service (WINS)** server, then sends a broadcast to request local name resolution. An M node broadcasts first, then attempts a directed request for name resolution. This approach reduces the amount of broadcast traffic on most IP-based networks that use NetBIOS names.

TCP/IP Advantages

As network protocols go, TCP/IP is not extremely fast or easy to use. However, TCP/IP supports networking services better than the other Windows 2000 protocols, through its multiple components (see Figure 7-1 and Table 7-1). TCP/IP supports multiple routing protocols that

can support large, complex networks. It also incorporates better error detection and handling, and works with more kinds of computers than any other protocol. The following is a list of the elements shown in Figure 7-1:

- *Other:* Any of the nearly 40 other service/application-level protocols defined for TCP/IP
- ***File Transfer Protocol (FTP)****:* The service protocol and corresponding TCP/IP application that permit network file transfer
- ***Telnet****:* The service protocol and corresponding TCP/IP applications that support networked terminal emulation services
- ***Simple Mail Transfer Protocol (SMTP)****:* The most common e-mail service protocol in the TCP/IP environment. (POP3, the Post Office Protocol version 3, and IMAP, the Internet Message Access Protocol, are also involved in a great deal of Internet e-mail traffic.)
- ***User Datagram Protocol (UDP)****:* A secondary transport protocol on TCP/IP networks, UDP is a lightweight cousin of TCP. It is **connectionless**, has low overhead, and offers best-effort delivery rather than the delivery guarantees offered by TCP. It is used for all kinds of services on TCP networks, including NFS and TFTP.
- ***Network File System (NFS)****:* A UDP-based networked file system originally developed by Sun Microsystems and widely used on many TCP/IP networks. (Windows 2000 does not include built-in NFS support, but numerous third-party options are available.)
- ***Trivial File Transfer Protocol (TFTP)****:* A lightweight, UDP-based alternative to FTP designed primarily to permit users running Telnet sessions elsewhere on a network to grab files from remote machines
- ***Domain Name Service (DNS)****:* An address resolution service for TCP/IP-based networks that translates between numeric IP addresses and symbolic names known formally as fully qualified domain names (FQDNs)
- ***Simple Network Management Protocol (SNMP)****:* The primary management protocol used on TCP/IP networks, SNMP is used to report management data to management consoles or applications and to interrogate repositories of management data around a network
- ***Transmission Control Protocol (TCP)****:* The primary transport protocol in TCP/IP, TCP is a robust, reliable, guaranteed delivery, **connection-oriented** transport protocol
- *Routing protocols:* These embrace a number of important IP protocols, including the Routing Internet Protocol (RIP), the Open Shortest Path First (OSPF) protocol, the Border Gateway Protocol (BGP), and others.
- ***Address Resolution Protocol (ARP)****:* Used to map from a numeric IP address to a MAC-layer address

- *Reverse Address Resolution Protocol (RARP):* Used to map from a MAC-layer address to a numeric IP address
- ***Internet Protocol (IP)****:* The primary protocol in TCP/IP, IP includes network addressing information that is manipulated when a packet is routed from sender to receiver, along with data integrity and network status information.
- ***Internet Control Message Protocol (ICMP)****:* The protocol that deals with quality of service, availability, and network behavior information; also supports the **PING (Packet Internet Groper)** utility often used to inquire if an address is reachable on the Internet
- *IEEE 802.X:* Includes the 802.2 networking standard, plus standard networking technologies such as Ethernet (802.3) and Token Ring (802.5), among others
- ***Asynchronous Transfer Mode (ATM)****:* A cell-oriented, fiber- and copper-based networking technology that supports data rates from 25 Mbps to as high as 2.4 Gbps
- *Fiber Distributed Data Interface (FDDI):* A 100 Mbps fiber-based networking technology.
- *Integrated Services Digital Network (ISDN):* A digital alternative to analog telephony, ISDN links support 2 or more 64-Kbps channels per connection, depending on type.
- *X.25:* An ITU standard for packet-switched networking, X.25 is very common outside the U.S., where its robust data-handling makes it a good match for substandard telephone networks.
- *Ethernet II:* An older version of Ethernet that preceded the 802.3 specification, Ethernet II offers the same 10 Mbps as standard Ethernet, but uses different frame formats.

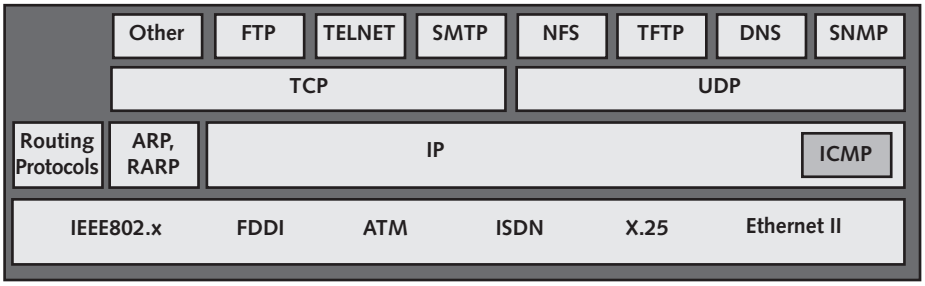

Figure 7-1 TCP/IP protocol stack

Table 7-1 Protocols in the Windows TCP/IP Stack

Protocol	Primary Function
Simple Network Management Protocol (SNMP)	Allows monitoring across host computers
Windows Sockets API	The standard interface between TCP/IP socket applications and protocols
NBT	NetBIOS over TCP/IP: Provides NetBIOS naming services
Transmission Control Protocol (TCP)	Provides connection-oriented services
User Datagram Protocol (UDP)	Provides connectionless services
Address Resolution Protocol (ARP)	Obtains hardware addresses for communication at the Network layer
Internet Protocol (IP)	Provides addressing and routing functions
Internet Control Message Protocol (ICMP)	Reports messages and errors regarding data delivery

In addition to its many services and capabilities, TCP/IP also supports the following:

- Direct Internet access from any TCP/IP-equipped computer with a link to the Internet, by phone, some kind of digital link (ISDN, frame relay, T1, and so forth), or across any network with routed Internet access
- Powerful network management protocols and services, such as SNMP and the Desktop Management Interface (DMI, which supports interrogation of desktop hardware and software configuration data)
- Dynamic Host Configuration Protocol (DHCP), which provides unique IP addresses on demand and automates IP address management
- Microsoft Windows Internet Naming Service (WINS) to enable IP-based NetBIOS name browsing for Microsoft clients and servers, as well as the Domain Name Service (DNS) that is the most common name resolution service used to map FQDNs to numeric IP addresses throughout the Internet

Unlike IPX/SPX, the InterNIC manages all TCP/IP domain names, network numbers, and IP addresses, to make the global Internet work reliably.

TCP/IP Drawbacks

For all the clear advantages of TCP/IP, there are some drawbacks. Configuring and managing a TCP/IP-based network requires a fair degree of expertise, careful planning, and constant maintenance and attention. Each of the many services and protocols that TCP/IP supports brings its own unique installation, configuration, and management chores. In addition, there's a huge mass of information and unforgiving detail work involved in establishing and maintaining a TCP/IP-based network. In short, it's a demanding and unforgiving environment, and should always be approached with great care.

Data Link Control

The **Data Link Control (DLC)** transport mechanism is not designed for connectivity between computers, as are the other transport protocols we discuss. Windows 2000 uses DLC to connect to IBM mainframes (via 3270 terminal emulation) or to access network-attached printers such as the HP 4si.

DLC offers only limited functionality as a network transport. It has been supplanted by TCP/IP in most networks because most direct-attached printers available today rely primarily on TCP/IP-based remote printing protocols. TCP/IP supports IBM host access protocols such as Tn3270 and Tn5250; these protocols not only provide better terminal emulation capabilities, but also are inherently routable and do not rely on extensive broadcast traffic, as does DLC.

DLC has the following disadvantages:

- It cannot support higher-level file transfer protocols (that is, it's good only for printing and terminal emulation, and that's all).
- It is not only unroutable, it's also hard to bridge.
- It is a simple, primitive network transport and is entirely unsuited for higher-level services.

Interprocess Communication (IPC)

In the Windows 2000 environment, communication among processes is quite important because of the operating system's multitasking, multithreaded architecture. **Interprocess communication (IPC)** defines a way for such processes to exchange information. This mechanism is general-purpose, so it doesn't matter whether such communications occur on the same computer or between networked computers. IPC defines a way for client computers to request services from some servers and permits servers to reply to requests for services. In Figure 7-2, IPC operates directly below the redirector on the client side and the network file system on the server side to provide a standard communications interface for handling requests and replies.

In Windows 2000, IPC mechanisms fall into two categories: programming interfaces and file systems. Programming interfaces permit general, open-ended client/server dialog as mediated by applications or system services. Normally, such dialog is not strictly related to data streams or data files. File systems support file sharing between clients and servers. Where programming interfaces are concerned, individual APIs differ depending on what kinds of client-server dialog they support. Where file systems are concerned, they must behave the same way, no matter how (or where) they employ Windows 2000 networked file systems and services.

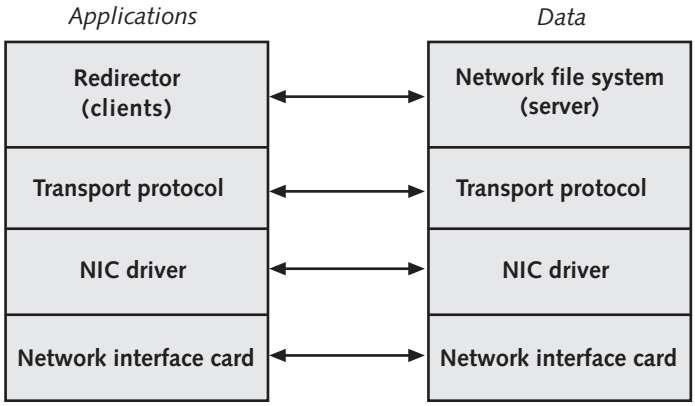

Figure 7-2 Interprocess communication between client and server

IPC File System Mechanisms

Windows 2000 includes two IPC interfaces for file system access: named pipes and mailslots. These mechanisms work through the Windows 2000 redirector, which distinguishes between local and network resource requests. This process permits one simple set of file I/O commands to handle both local and network access to file system data.

Named Pipes

Named pipes support a connection-oriented message-passing service for clients and servers. To be connection-oriented, a message's receiver must acknowledge each message received. Named pipes offer a reliable method for clients and servers to exchange requests, replies, and associated files. Named pipes provide their own methods to ensure reliable data transfer, which makes them a good match for lightweight, unreliable transport protocols such as the User Datagram Protocol. In short, named pipes delivery guarantees make transport-level delivery guarantees less essential.

The Windows 2000 version of named pipes includes a security feature called impersonation, which permits the server side of the named pipes interface to masquerade as a client that requests a service. This allows the interface to check the client's access rights and to make sure that the client's request is legal, before returning any reply to a request for data.

Mailslots File System

Mailslots are like a connectionless version of named pipes; mailslots offer no delivery guarantees, nor do they acknowledge the successful receipt of data. Windows 2000 uses mailslots as an internal method of supporting nonessential system-to-system communications. Such things as registering names for computers, domains, and users across a network, passing messages related to the Windows 2000 browser service, and providing support for broadcasting text messages across the network fall into this category. Except for such lightweight uses, mailslots are used less frequently than named pipes.

IPC Programming Interfaces

For communications to succeed, the client and server sides of an application must share a common programming interface. Windows 2000 offers a number of distinct interfaces to support IPC mechanisms for various kinds of client/server applications. Windows 2000 supports several programming interfaces, including NetBIOS, Windows Sockets, RPC, and NetDDE.

External applications can support other programming interfaces or implement private interfaces.

NetBIOS

NetBIOS is a widely used but simple PC client/server IPC mechanism. Because it is so easy to program, it has remained quite popular ever since IBM published its definition in 1985. NetBIOS services are required to permit a Microsoft Windows network to operate. Fortunately, NetBIOS works with all TDI-compliant transports, including NetBEUI (NBF), NWLink (NWLink over NetBIOS or NWNBLink), and TCP/IP (NBT).

Windows Sockets (WinSock)

Windows Sockets (WinSock) defines a standardized and broadly deployed interface to network transports such as TCP/IP and IPX. WinSock was created to migrate UNIX applications written to the Berkeley Sockets specification to the Windows environment. WinSock also makes it easier to standardize network communications used on multiple platforms, because one socket interface is much like another, even if one runs on UNIX and the other on some variety of Windows (such as Windows 2000, where WinSock 2.0 is becoming the standard sockets API).

WinSock appears in many programs that originated as UNIX programs, including the majority of Internet utilities, especially the most popular IP utilities, such as Web browsers, e-mail software, and file transfer programs.

Remote Procedure Call (RPC)

Remote Procedure Call (RPC) implements IPC tools that can invoke separate programs on remote computers, supply them with input, and collect whatever results they produce. This permits the distribution of a single processing task among multiple computers, a process that can improve overall performance and help balance the processing load across numerous machines.

RPC is indifferent to where its client and server portions reside. It's possible for both client and server portions of an application to run on a single computer. In that case, they will communicate using local procedure call (LPC) mechanisms. This makes building such applications easy because they can be constructed on one computer, while allowing processing to be distributed on one machine or across many machines, as processing needs dictate. This creates an environment that is both flexible and powerful.

RPC consists of four basic components:

- A remote stub procedure that packages RPC requests for transmission to a server. It's called a stub because it acts as a simple, extremely compact front end to a remote process that may be much larger and more complex elsewhere on the network.
- An RPC run-time system to pass data between local and remote machines or between client and server processes.
- An application stub procedure that receives requests from the run-time RPC system. Upon such receipt, this stub procedure formats requests for the designated target RPC computer and makes the necessary procedure call. This procedure call can be either a local procedure call (if both client and server components are running on the same computer) or a remote procedure call (if client and server components are running on two machines).
- One or more remote procedures, which may be called for service (whether locally or across the network).

NetDDE

Network Dynamic Data Exchange (NetDDE) creates ongoing data streams called exchange pipes (or simply pipes) between two applications across a network. This process works just like Microsoft's local **Dynamic Data Exchange** (**DDE)**, which creates data exchange pipes between two applications on the same machine. DDE facilitates data sharing, object linking and embedding (OLE), and dynamic updates between linked applications. NetDDE extends local DDE across the network.

NetDDE services are installed by default during the base Windows 2000 installation, but they remain dormant until they are explicitly started. NetDDE services must be started using the Services control in Computer Management, where they appear under the headings Network DDE (the client side of NetDDE) and Network DDE DSDM (DDE Share Database Manager, the server side of NetDDE).

Distributed Component Object Model (DCOM)

DCOM (previously known as "Network OLE") is a protocol that facilitates the communication of application components over a network by providing a reliable, secure, and efficient mechanism for exchanging information. DCOM can operate over most network transport mechanisms, including HTTP. Microsoft based its implementation of DCOM on the Open Software Foundation's DCE-RPC specification, but expanded its capabilities to include Java and ActiveX support.

Windows Network (WNet) Interface

The WNet interface allows applications to take advantage of Windows 2000 networking capabilities through a standardized API. This means that the application does not require specific control data about the network provider or implementation, allowing applications to be network-independent while still able to interact with network-based resources.

Win32 Internet API (WinInet)

The WinInet API is a mechanism that enables applications to take advantage of Internet functionality without requiring extensive proprietary programming. Via WinInet, applications can be designed to include FTP, Web, and Gopher support with a minimum of additional coding. WinInet makes interacting with Internet resources as simple as reading files from a local hard drive, without requiring programming to WinSock or TCP/IP.

REDIRECTORS

A **redirector** examines all requests for system resources and decides whether such requests are local (they can be found on the requesting machine) or remote. The redirector handles transmission of remote requests across the network so that the requests are filled.

Windows 2000 file and print sharing are regarded as the most important functions supplied by any network operating system. Windows 2000 delivers these services through two critical components: the Workstation service and the Server service. Both of these services are essentially file system drivers that operate in unison with other file system drivers that can access local file systems on a Windows 2000 machine. The following components are redirectors that operate at this level:

- Workstation service
- Server service
- Multiple Universal Naming Convention Provider (MUP)
- Multi-Provider Router (MPR)

All of these system components take client requests for service and redirect them to an appropriate network service provider. Redirectors interact and interface directly with user applications. The sections that follow explain more about each of these components and their roles in the Windows 2000 networking environment.

Workstation Service

The **Workstation service** supports client access to network resources and handles functions such as logging in, connecting to network shares (directories and printers), and creating links using the Windows 2000 IPC options. The Workstation service has two elements, the User mode interface and the redirector. The User mode interface determines the particular file system that any User mode file I/O request is referencing. The redirector recognizes and translates requests for remote file and print services and forwards them to lower-level **boundary layers** aimed at network access and delivery.

This service encompasses a redirector file system that handles access to shared directories on networked computers. The file system is used further to satisfy remote access requests, but if any request uses a network name to refer to a local resource, it will pass that request to local file system drivers instead.

The Workstation service requires that at least one TDI-compliant transport and at least one MUP are running. Otherwise, the service cannot function properly because it supports connections with other Windows 2000 machines (through their Server services), LAN Manager, LAN Server, and other MS-Net servers, which require a MUP to be running. The Workstation service, like any other redirector, communicates with transport protocols through the common TDI boundary layer.

Server Service

The Windows 2000 **Server service** handles the creation and management of shared resources and performs security checks against requests for such resources, including directories and printers. The Server service allows a Windows 2000 computer to act as a server on a client/server network, up to the maximum number of licensed clients. This limits to 10 the number of simultaneous connections possible to a Windows 2000 Professional machine, in keeping with its built-in connection limitations.

Just as with the Workstation service, the Server service operates as a file system driver. Therefore, it also uses other file system drivers to satisfy I/O requests. The Server service is also divided into two elements:

- *Server.exe:* Manages client connection requests.
- *Srv.sys:* The redirector file system that operates across the network, and that interacts with other local file system drivers when necessary.

Multiple Universal Naming Convention Provider (MUP)

Windows 2000 supports multiple redirectors that can be active simultaneously. As an example, both the Workstation and Server services and the NetWare redirector built into the Windows 2000 **Client Service for NetWare (CSNW)** can be active at the same time. Like the Server service, the NetWare redirector handles Microsoft Windows network shares, but exposes them to NetWare clients instead of Microsoft network clients. The ability to support multiple clients uniformly is possible because a common provider interface allows Windows 2000 to treat all redirectors the same way.

The **Multiple Universal Naming Convention Provider (MUP)** defines a link between applications that make UNC requests for different redirectors. MUP allows applications to remain oblivious to the number or type of redirectors that might be in use. For incoming requests, the MUP also decides which redirector should handle that request by parsing the UNC share name that appears within the request.

Here's how the MUP works: When the I/O subsystem receives any request that includes a UNC name, it turns that request over to the MUP. The MUP first checks its internal list of recently accessed shares, which it maintains over time. If the MUP recognizes the UNC name, it immediately passes the request to the required redirector. If it doesn't recognize the UNC name, the MUP sends the request to each registered redirector and requests that it service the request.

The MUP chooses redirectors on the basis of the highest registered response time during which the redirector claims it can connect to a UNC name, information that can be cached until no activity occurs for 15 minutes. This can make trying a series of redirectors incredibly time-consuming and helps explain why the binding order of protocols is so important, because that also influences the order in which name resolution requests will be handled.

Universal Naming Convention Names

Universal Naming Convention (UNC) names represent the format used in NetBIOS-oriented name resolution systems. UNC names precede the computer portion of a name with two slashes, followed by a slash that precedes (and separates elements of) the share name and the directory path, followed by the requested filename. Thus the following string:

```
\\computername\sharename\dir-path\filename.ext
```


represents a valid UNC name. In this example the name of the computer is "computername," the name of the share is "sharename," the directory path is "dir-path," and the file is named "filename.ext."

Multi-Provider Router (MPR)

Not all programs use UNC names in the Windows 2000 environment. Programs that call the Win32 API must use a file system service called the **Multi-Provider Router (MPR)** to designate the proper redirector to handle a resource request. The MPR lets applications written to older Microsoft specifications behave as if they were written to conform to UNC naming. The MPR is able to recognize the UNCs that represent drive mappings, so it can decide which redirector can handle a mapped network drive letter (such as X:) and make sure that a request that references that drive can be properly satisfied.

The MPR handles all Win32 network API calls, passing resource requests from that interface to those redirectors that register their presence through special-purpose dynamic link libraries (DLLs). That is, any redirector that wants to support the MPR must provide a DLL that communicates through the common MPR interface. Normally this means that whichever network developer supplies a redirector must also supply this DLL. Microsoft implemented CSNW as a DLL that supports this interface. This allows the NetWare redirector to provide the same kind of transparent file system and network resource access as other Windows 2000 redirectors.

Networking Under Windows 2000

The Windows 2000 networking system is controlled by a single multifaceted interface that combines networking access for LAN, Internet, and modem. The interface is called Network and Dial-up Connections (see Figure 7-3). It is accessed through the Settings entry in the Start menu or through the My Computer, Control Panel display.

Adding new network interface cards (NICs) to Windows 2000 Professional is handled in the same fashion as installing any other piece of hardware—physically install it, allow

Windows 2000 Plug and Play to detect it, and install the appropriate driver(s), or use the Add/Remove Hardware applet to manually install the device. Both of these procedures are discussed in Chapter 3. Once a new NIC is installed, Windows 2000 automatically creates a new Local Area Connection icon, which you can use to customize the settings for your networking needs.

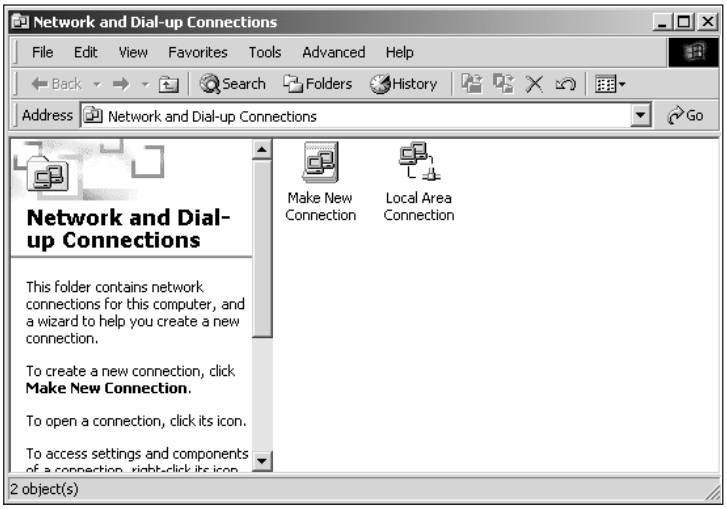

Figure 7-3 Network and Dial-up Connections dialog box

Network and Dial-up Connections is an Internet Explorer-based tool used to create and configure network connections. The Make New Connection icon links to a wizard that takes the user through the process of establishing new network links. The wizard is used for any network links employing modems, virtual private networks (VPNs) over the Internet, or serial, parallel, or infrared ports. Windows 2000 automatically enables all "normal" network links achieved through a network adapter and an attached cable. A Local Area Connection icon is listed in the Network and Dial-up Connections window for each installed adapter. If there are two or more LAN connections, rename the Local Area Connection icons to reflect the domain, network, or purpose of the link. (Try Hands-on Project 7-1 to view the status of a local area connection.)

Existing Local Area Connections can be configured by opening the Properties for that object either via the File menu or the right-click menu. A typical default configuration of a Local Area Connection Properties dialog box is shown in Figure 7-4, listing the adapter in use as well as all installed protocols and services that can function over this interface. The Configure button is used to access the Properties dialog box for the adapter. Each listed service or protocol has a check box. When checked, the protocol or service is bound to the adapter (that is, it can operate over the network link established by the adapter). When unchecked, the protocol of service is not bound to the adapter.

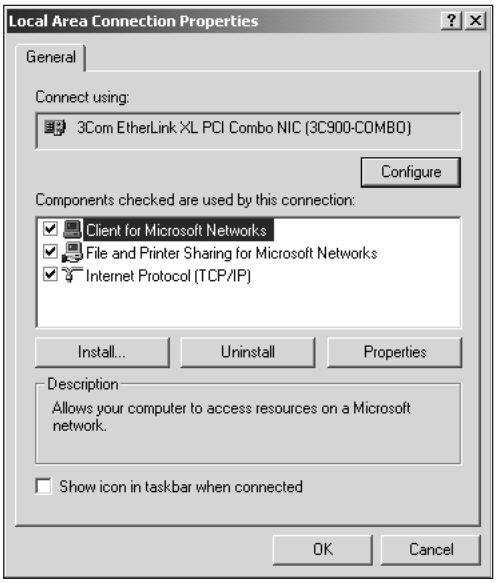

Figure 7-4 A Local Area Connection Properties dialog box

The Install button is used to add new client interfaces, protocols, and services that any of the Connection objects can use. When a new element is added, all possible bindings are enabled by default. The following are the additional networking elements (not including the default elements listed in Figure 7-4) that can be installed in Windows 2000 Professional:

- *Client: Client Service for NetWare*—Used to gain access to NetWare resources (see Chapter 8)
- *Service: QoS Packet Scheduler*—An extension service for WinSock used to reserve bandwidth for communications
- *Service: SAP Agent*—Used by Windows 2000 to participate actively in NetWare networks (see Chapter 8)
- *Protocol: AppleTalk Protocol*—Used to access Macintosh-hosted printers
- *Protocol: DLC Protocol*—Used to access network attached printers or IBM mainframes
- *Protocol: NetBEUI Protocol*—Nonroutable protocol
- *Protocol: Network Monitor Driver*—Driver used to allow full versions of Network Monitor to obtain network activity information from Windows 2000 Professional systems
- *Protocol: NWLink IPX/SPX/NetBIOS Compatible Transport Protocol*—Protocol most often used on NetWare networks (see Chapter 8)

The Uninstall button is used to remove a client, protocol, or service. Once an element is removed, it is removed for all Connection objects. The Properties button opens the Properties dialog box for the selected installed component (client, service, or protocol). (Not all components have configurable options.) This dialog box also offers a check box control to display an icon in the icon tray when the Connection object is in use.

The Network and Dial-up Connections interface File and Advanced drop-down menus include the following functions:

- *File: Disable*—Prevents the selected Connection object from being used to establish a communications link. This command is for automatic connections, such as those for a LAN.
- *File: Enable*—Allows the selected Connection object to be used to establish a communications link. This command is for automatic connections, such as those for a LAN.
- *File: Connect*—Launches the selected Connection object to establish a communications link. This command is for manual connections, such as those over a modem.
- *File: Status*—Displays a Status window for the selected Connection object that lists whether the object is connected, how long the connection has been active, the speed of the connection, and packet counts. This window offers Properties and Disable buttons to perform the same functions as the File menu commands.
- *File: New Connection*—Launches the Make New Connection Wizard
- *File: Create Copy*—Creates a duplicate copy of the selected Connection object
- *File: Create Shortcut*—Creates a shortcut to the selected Connection object
- *File: Delete*—Removes the selected Connection object
- *File: Rename*—Changes the name of the selected Connection object
- *File: Properties*—Opens the Properties dialog box for the selected Connection object
- *File: Close*—Exits the Network and Dial-up Connection interface
- *Advanced: Operator-Assisted Dialing*—Used to manually dial a connection number and then have the computer take control of the line once the remote system answers the call
- *Advanced: Dial-up Preferences*—Opens a dialog box in which RAS-related controls are set (see Chapter 9)
- *Advanced: Network Identification*—Opens the Network Identification tab of the System applet that displays the current computer name and workgroup/domain name. To join a domain and create a local user, click Network ID.
- *Advanced: Advanced Settings*—Opens a dialog box where bindings and provider order can be managed. See the "Managing Bindings" section later in this chapter.

- *Advanced: Optional Networking Components*—Used to add other networking components such as Monitoring and Management Tools, Networking Services, and Other Network File and Print Services

Some of these commands appear only when a specific Connection object type is selected.

For most networks, the default Local Area Connection that Windows 2000 creates automatically is sufficient for LAN activity. As shown earlier in Figure 7-4, this Connection object is designed to link up with a Microsoft-based network (workgroup or domain), allows file and printer sharing, and employs the TCP/IP protocol.

To change the TCP/IP settings, select the protocol from the list of components in the Properties window of a Local Area Connection, then click Properties. This reveals the Internet Protocol (TCP/IP) Properties dialog box (see Figure 7-5). From here, you can easily enable DHCP for this computer, or define a static IP address, subnet mask, and gateway. You can also define the preferred and alternate DNS servers. The Advanced button brings up a multitabbed dialog box in which multiple IP addresses, additional gateways, DNS and WINS functionality, and TCP/IP service extension properties can be defined.

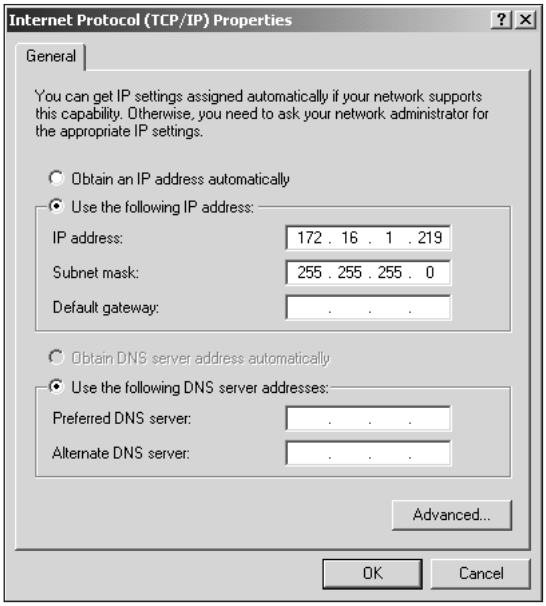

Figure 7-5 The Internet Protocol (TCP/IP) Properties dialog box

MANAGING BINDINGS

Binding refers to the order in which Windows 2000 networking components are linked. These linkages and the order in which multiple components are linked affect how the systems behave and how well they perform. Binding is defined in the Advanced Settings dialog box (see Figure 7-6). This dialog box is reached by clicking the Advanced Settings command from the Advanced menu of the Network and Dial-up Connections window. (You can view network bindings in Hands-on Project 7-5.)

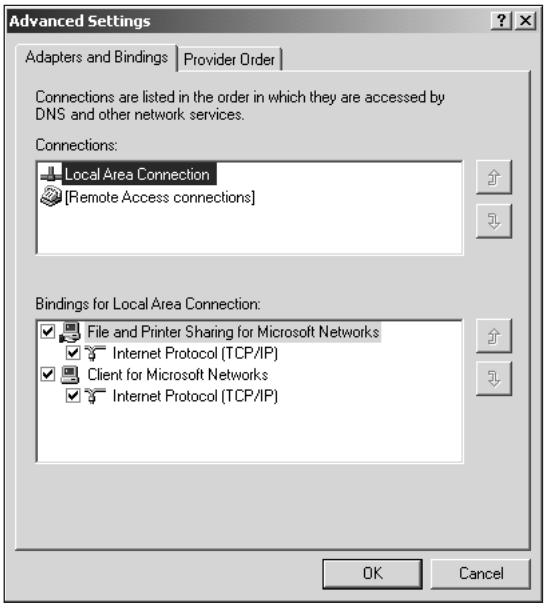

Figure 7-6 The Advanced Settings dialog box, Adapters and Bindings tab

By default, Windows 2000 binds any two components that share a common boundary layer, unless such bindings are explicitly removed. In fact, Windows 2000 binds all components that share a common boundary to the boundary layer they share, unless one or more of these bindings is removed manually.

Because this default is what is called "complete binding"—that is, all possible bindings are created—it can lead to system inefficiencies, especially when bindings are created that will not be used. Such unused bindings might appear higher in the binding order than bindings that are used. This arrangement can build delays into the system because the MUP attempts to satisfy UNC requests for names it does not recognize in the order in which bindings appear, and unused bindings must time out before the next binding in the order is attempted.

Disabling all protocol bindings that are not needed or used improves system performance and decreases the likelihood of communication errors. If remote access with NetBEUI is not required, disable the binding between the NetBEUI transport and the Remote Access WAN

Wrapper (it appears as a "virtual" adapter in the bindings list). It's also important to understand that because clients (in this case Windows 2000 Professional machines) initiate communications with Windows 2000 Servers, changing the binding order of protocols on clients is what matters. Servers respond using whatever protocol requests appear within the transmission, so changing their binding order won't do much to improve performance. Changing a client's binding order, on the other hand, can sometimes deliver dramatic performance improvements.

Binding priority affects network performance because Windows 2000 makes connections according to the order in which protocols are bound. For two machines that use NetBEUI and TCP/IP, Windows 2000 uses whichever protocol appears higher in the services binding list. If both computers run NetBEUI and TCP/IP, and NetBEUI ranks higher than TCP/IP in the binding list, they will establish a faster connection (NetBEUI is faster than TCP/IP) than if the bindings were reversed. To change the priority for any transport protocol, highlight an object on the Adapters and Bindings tab, then use the arrow buttons to increase or decrease its priority level. You can also unbind services and protocols by unselecting the check box in front of the object's name.

The Provider Order tab is used to alter the binding priority of various providers, such as network connectivity or print servers. This is useful only when two or more providers of the same type can be employed by a system. For example, if a computer can participate in NetWare and Windows 2000 networking environments, it can be useful to change the priority of the providers to favor the most often accessed network.

TCP/IP Architecture

TCP/IP supports easy cross-platform communications and provides the technical foundation for the Internet. TCP/IP is actually a suite of protocols; in this discussion, we break it down into IP and TCP. Under each of these protocols lie many additional protocols that give the TCP/IP suite such a wide range of functionality.

Internet Protocol

The Internet Protocol (IP) provides source and destination addressing and routing in the TCP/IP suite. IP addresses are logical addresses that are 32 bits (4 bytes) long. Each byte, or octet, is represented by a decimal number from 0 to 255 and separated from the others by a period, for example, 183.24.206.18. IP is a connectionless datagram protocol that, like all connectionless protocols, is fast but unreliable. IP assumes that other protocols will be available to ensure reliable delivery of the data.

Although 8 bits have 256 possible combinations, the numbers 0 and 255 are reserved for special purposes. In the range of 0–255, the zero address is reserved to identify the network, and the 255 address is used for broadcasts that are read by all IP hosts on the network. IP network hosts can use only numbers 1 through 254. "Host" is the IP-specific term that identifies any device on an IP network that is assigned a specific address.

Part of the IP address assigned to a computer designates which network the computer is on, and the remainder of the address represents the host ID of that computer. The 4 bytes that IP uses for addresses can be broken up in multiple ways; in fact, several classes of IP addresses have been defined that use different boundaries for the network part and the host ID part. These are shown in Table 7-2.

Table 7-2 Classes of IP Addresses

Class	Network IDs	Host IDs	Usable Network IDs
A	126	16,777,214	1–126
B	16,328	65,534	128.1–191.255
C	2,097,150	254	192.0.1–223.255.254

In a Class A address, the first octet is used to identify the network, and the three trailing octets are used to identify the hosts. This creates a situation in which a small number of networks (126, to be exact) is possible, but a large number of hosts (over 16 million per network) can be defined on each one. Class B addresses split the octets evenly, so the first two identify the network and the second two identify the host. This permits over 16,000 networks with over 65,000 hosts. Class C addresses use the first three octets for the network portion of an address and the final octet for the host portion. This permits over two million networks, but only a maximum of 254 hosts for each Class C network.

For example, if a computer has an address of 183.24.206.18, this indicates that it is a Class B address because the first two octets fall in the range of 128.1-191.255, as indicated in the fourth column of Table 7-2. Thus, the first two octets represent the network address (183.24), and the host address portion is 206.18. The computer next to it might have the address of 183.24.208.192, which indicates that it's on the same network (183.24) but has a different host address (208.192).

IP uses a special bit mask called a **subnet mask** to determine which part of an address denotes the network and which part the host. The job of the subnet mask is to block out the host section of the address so that only the network ID portion remains significant. For the addresses on the 183.24 network, the subnet mask can be stated as 255.255.0.0. Notice that the two most significant octets are occupied by a binary value that translates into all ones (255 is 11111111 in binary), whereas the host portion is all zeros (0 is the same as 00000000 in binary).

Sometimes IP network administrators use part of what the IP address class considers the host portion of an address to further subdivide a single Class A, B, or C network. You might see the occasional subnet mask that looks like 255.192 for a Class A network, 255.255.192 for a Class B network, and 255.255.255.192 for a Class C network. 192 equals 11000000 in binary, so this extends the network portion two digits into the host ID portion of the address and permits defining two subnets within a single range of host addresses. The top and bottom values (0 and 3, in this case) are reserved to identify the subnetwork and to handle broadcasts, respectively.

Another form of addressing is increasingly used on IP networks, especially when individual networks don't need, or can't use, an entire Class B or Class C address. This technique is called Classless Interdomain Routing (CIDR), pronounced "cider".) CIDR uses the same technique described in the preceding paragraph to let Internet service providers (ISPs) subdivide their available addresses into more numerous subnetworks and make better use of the IP address space that's still available.

All TCP/IP addresses must be unique on the Internet—and in fact, on any IP-based network. If two IP addresses are identical, neither machine with that address will be able to access the network. That's why managing IP addresses is quite important. At present, this responsibility falls under the aegis of the InterNIC. All the Class A addresses were handed out years ago, most Class Bs have been allocated, and Class C addresses are becoming scarce. (When you add all possible networks allowed by all three address classes, you get the maximum number of individual networks on the Internet as 2,113,604). Given the vast number of networks on the Internet and the continuing growth in that arena, it is clear that subnet masking tricks and CIDR merely represent stopgap measures to extend the current address space as much as possible. At the same time, the standards body that governs the Internet (the IAB, or Internet Activities Board) is working to complete a new version of TCP/IP called IPv6 (the current version is IPv4) that will extend the address space significantly. (The address space expands to 128 bits with IPv6, as compared to the current 32 bits; this is enough to support trillions of networks with trillions of nodes per network.)

All IP-based devices on a single network segment must use the same subnet mask.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) is used to send control messages (such as error messages, quality of service information, and confirmations) between IP hosts. PING is used to request a response from a remote host. It uses ICMP to return messages regarding this function, such as whether the response was received or timed out, or the host was not reachable. (PING is covered in more detail in a later section.)

Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is used to associate a logical (IP) address to a physical (MAC) address. When a system begins a conversation with a host for which it does not have a physical address, the system sends an ARP broadcast packet requesting a physical address that corresponds to the logical address. Given this information, the packet can be correctly sent across a physical network.

Ethernet is the common form of network in use, and on most networks the MAC address is identical to the Ethernet address. The Ethernet or M address is a 48-bit address normally represented as 12 hexadecimal digits. In other words, on an Ethernet network the physical address or MAC address is the same as the Ethernet address burned into PROM on the network interface card that attaches a computer to a network. On other types of networks, the interfaces also supply unique MAC layer addresses, but their formats vary according to the kind of network in use.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is used to automatically configure computers. A DHCP server manages a defined block of IP addresses that can be assigned to computers upon request. Network devices basically take out a lease on an address, and can use that address only so long as the lease remains valid. The DHCP server handles granting, renewing, or canceling such leases. It can also block out reserved IP addresses within a numeric range, permitting certain computers (which may not be able to communicate with the DHCP server) to use static, fixed IP address assignments.

Using DHCP makes it easy for network administrators to manage IP addresses, and makes it more or less automatic for users to gain access to IP-based resources. DHCP has proven to be a real boon for those reasons, and one of the best features of Windows 2000 is that it can be configured for TCP/IP by selecting a single radio button on the IP Protocol Properties dialog box that reads "Obtain an IP address automatically."

Transmission Control Protocol

Transmission Control Protocol (TCP) is the primary Internet transport protocol. It accepts messages of any length and provides transport to a TCP peer on a remote network host. TCP is connection-oriented, so it provides more reliable delivery than connectionless-oriented IP. When a connection is established, a TCP port number is used to determine which process on the designated host is to receive any particular packet. TCP is responsible for message fragmentation and reassembly. It uses a sequencing function to ensure that packets are reassembled in the correct order, and includes mechanisms both to acknowledge successful delivery of correct packets and to request retransmission of damaged or lost packets.

UDP

User Datagram Protocol (UDP) is a connectionless protocol. As a result of its reduced overhead, it is generally faster, although less reliable, than TCP. UDP was designed primarily to transport purely local services, where it is relatively safe to assume network reliability. This is one reason why it's used for distributed file systems like the Network File System (NFS) and for the Trivial File Transfer Protocol (TFTP), where the underlying assumption is that access is either purely local (NFS) or that guaranteed delivery is not required (TFTP).

FTP

File Transfer Protocol (FTP) provides file transfer services, as well as directory and file manipulation services, such as listing directory contents, deleting files, and specifying file formats.

A command-line version of FTP is available as part of Windows 2000. To learn more about this command, open a Command Prompt window (Start, Programs, Accessories, Command Prompt) and enter *FTP* at the command line, then enter *?*. This produces the Help file for FTP.

Telnet

Telnet is a remote terminal emulation protocol that is primarily used to provide connectivity between dissimilar systems (PC and VAX/VMS, PC and router, UNIX and VMS), where the remote client works on the Telnet host machine as if it were a terminal attached directly to that host. Using Telnet, remote equipment, such as routers and switches, can be monitored and configured, or remote systems can be operated as needed. Despite a primitive, character-oriented interface, Telnet remains one of the most important IP services.

A 32-bit windowed version of Telnet is available as part of Windows 2000. To learn more about this utility, launch Telnet (execute *Telnet* from a Start, Run command) and access its Help utility.

SMTP

Simple Mail Transfer Protocol (SMTP) is used to provide IP-based messaging services. Although it is not the only e-mail protocol available in the IP environment, most experts regard SMTP as the basis for Internet e-mail.

SNMP

Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for network management. SNMP is an industry-standard protocol supported by most networking equipment manufacturers. SNMP can query collections of management data, called management information bases (MIBs), on networked devices. This permits management applications to use SNMP to poll devices on the network and obtain regular status updates about their operating conditions, network utilization, and quality of service.

In addition, SNMP supports a "trap" mechanism that permits networked devices to send a message to a management application when specific events or error conditions occur. This capability is quite important because it permits networked devices to report potential or actual problems as soon as they're detected, rather than waiting for a management application to poll the device.

SNMP services are not activated by default on Windows 2000. To enable these services, use the Optional Networking Components command from the Advanced menu of the Network and Dial-up Connections interface.

The Berkeley R Utilities

Among the many enhancements added to the UNIX TCP/IP implementation present in the Berkeley Software Distribution (BSD) in the 1980s was a collection of IP-based network commands collectively known as the "R utilities," where the "R" stands for remote. This includes such commands as **rsh (remote shell)**, which permit a user on one network host to access shell commands on another network host, and **rexec (remote execution)**, which permits a user on one network host to execute a program remotely on another network host. Windows 2000 Professional supports both of these R utilities from the client side (but cannot act as a rsh or rexec server to other machines elsewhere on the network).

To learn more about rsh and rexec, open a Command Prompt window (Start, Programs, Accessories, Command Prompt) and enter either *rsh ?* or *rexec ?* to access the Help files for these command-line utilities.

PING

Packet Internet Groper (PING) is one of the most colorful acronyms in the TCP/IP utility box. PING is a command-line utility that uses the ICMP protocol to inquire if a designated host is reachable on the network. It also provides information about the round-trip time required to deliver a message to that machine and receive a reply. (Try using PING in Hands-on Project 7-2 at the end of the chapter.)

PING is a very useful utility that permits you to see if your own machine is properly attached to the network. You can PING yourself by entering the command PING 127.0.0.1 or PING loopback; in the latter case, this special address is defined as the loopback address, or the address of your own machine. You can find out if the network itself is working (by PINGing a nearby machine). Finally, you can determine if a particular machine is reachable (by PINGing either its host name or the equivalent numeric IP address). All of this capability comes in handy when you are installing and testing IP on a new machine or when you need to troubleshoot a network connection.

To learn more about PING, launch a Command Prompt window (Start, Programs, Accessories, Command Prompt) and enter PING (with no arguments) to access its online Help file. Note that PING can supply all kinds of routing and quality of service data, as well as simply test for reachability.

TFTP

Trivial File Transfer Protocol (TFTP) is a lightweight analog of FTP that uses UDP as its transport protocol rather than TCP. TFTP is a more stripped-down version of file transfer services than FTP; it basically supports the ability to communicate with a TFTP server elsewhere on the network and to copy files from the workstation to a remote host, or vice versa. For directory navigation, file grooming, or format translations, FTP is a much better choice.

To learn more about TFTP, open a Command Prompt window (Start, Programs, Accessories, Command Prompt), and enter *TFTP ?* to view its online Help file.

The HOSTS File

The **HOSTS** file is a static file placed on members of a network to provide a resolution mechanism between host names and IP addresses. The HOSTS file was the name resolution mechanism used before DNS was created. HOSTS files are used only on small networks where the deployment of a DNS server is unwarranted or for remote systems to reduce traffic over slow WAN links. Each line of a HOSTS file contains an IP address followed by one or more corresponding host names to that IP address. A system processes the HOSTS file on a line-by-line basis when attempting to resolve a host name. Once the first match is reached, the resolution process terminates and the acquired IP address is used. HOSTS files are only as useful as they are current. Most administrators update their HOSTS file on a regular basis and have a logon script automatically download the HOSTS file from a central location to remote systems each time they log on to the network.

Windows 2000 includes a sample HOSTS file in the %systemroot%\System32\drivers\etc folder. The HOSTS file is a plain text document that can be edited with Notepad or any other text editor. Basic information about editing the HOSTS file is included in its own header text, but for complete information consult the *Windows 2000 Resource Kit*.

DNS

Domain Name Service (DNS) is a critical component of the Internet's ability to span the globe. DNS handles the job of translating a symbolic name such as *lanw02.lanw.com* into a corresponding numeric IP address (172.16.1.7). It can also provide reverse lookup services to detect machines that are masquerading as other hosts. (A reverse lookup obtains the symbolic name that goes with an IP address; if the two do not match, the DNS server may assume that some form of deception is at work.)

DNS is a powerful, highly distributed database that organizes IP names (which for its purposes must take the form of fully qualified domain names) into hierarchical domains. When a name resolution request occurs, all the DNS servers that can identify themselves to each other cooperate very quickly to resolve the related address. DNS servers include sophisticated caching techniques that permit them to store recently requested name-address pairs, so that users can get to a previously accessed address quickly.

Windows 2000 Professional can communicate with DNS servers, but only Windows 2000 Server supports a full-fledged DNS server implementation.

The LMHOSTS File

The **LMHOSTS** file is a static file placed on members of a network to provide a resolution mechanism between NetBIOS names and IP addresses. The LMHOSTS file was the name resolution mechanism used before WINS was created. Now LMHOSTS files are used only on small networks where the deployment of a WINS server is unwarranted or for remote systems to reduce traffic over slow WAN links. Each line of an LMHOSTS file contains an IP address followed by the corresponding NetBIOS name. A system processes the LMHOSTS file on a line-by-line basis when attempting to resolve NetBIOS names. Once the first match is reached, the resolution process terminates and the acquired IP address is used. LMHOSTS files are only as useful as they are current. Thus, most administrators update their LMHOSTS file on a regular basis and have a logon script automatically download the LMHOSTS file from a central location to remote systems each time they log on to the network.

Windows 2000 includes a sample LMHOSTS file in the %systemroot%\System32\drivers\etc folder, which is named Lmhosts.sam. The LMHOSTS file is a plain text document that can be edited with Notepad or any other text editor. (Try Hands-on Project 7-3 to view the LMHOSTS sample file.) Basic information about editing the LMHOSTS file is included in its own header text, but for more information consult the *Windows 2000 Resource Kit*.

WINS

The Windows Internet Naming Service (WINS) is not a true "native" TCP/IP service; it is an extension added by Microsoft. As previously discussed, most of the internal and network communications within a Microsoft network employ NetBIOS. On a TCP/IP network, NetBIOS names must be resolved into IP addresses so packets can be properly delivered to the intended recipient. This process is automated by WINS. WINS dynamically associates NetBIOS names with IP addresses and automatically updates its database of associations as systems enter and leave a network, so it does not require ongoing maintenance. WINS is the dynamic service that is used to replace the static mechanism of the LMHOSTS file.

TCP/IP Configuration

TCP/IP configuration is performed through the Network and Dial-up Connections interface. When configuring TCP/IP for Windows 2000 Professional, there are many items of information that you need to know. If the machine uses DHCP, the DHCP server handles all these details. If not, here's a list of items that you might need to obtain from a network administrator (or figure out for yourself, if that's your job):

- A unique IP address for the computer
- The subnet mask for the network to which the computer belongs
- The address of the default gateway, the machine that attempts to forward any IP traffic not aimed at the local subnet (which makes it the gateway to other networks)

- The address of one or more DNS servers, to provide IP name resolution services. This is more important on bigger networks than on smaller ones. If you use an ISP for network access, you'll probably need to get this address from them.
- On Windows 2000 or Windows NT networks in particular, and IP-based Microsoft networks in general, you might need to provide an address for a WINS server. This permits NetBIOS name resolution requests to be transported across IP networks (even through routers if necessary).

When TCP/IP is installed, its default settings are to seek out a DHCP server to provide all configuration settings. If a DHCP server is already present on your network, you do not need to configure TCP/IP to be able to access the network.

TCP/IP configuration takes place in the Internet Protocol (TCP/IP) Properties dialog box (refer to Figure 7-5). Access the dialog box by clicking the Properties button after selecting TCP/IP from the list of installed components from the Properties dialog box of a Local Area Connection from the Network and Dial-up Connections interface. On a multihomed system (a computer with more than one network interface card) the configuration for each adapter can be different. Be sure to select the correct Local Area Connection object for the adapter you wish to modify. (You can practice step-by-step configuration of TCP/IP in Hands-on Project 7-4.)

There are two ways to assign an IP address to a computer: manually or via DHCP. As discussed earlier, DHCP is used to automatically configure the TCP/IP settings for a computer. If a DHCP server is available and will be used to configure this computer, select the "Obtain an IP address automatically" option. If there is no DHCP server available or if the configuration is to be handled manually, select the "Use the following IP address" option.

Before you can do this, however, you must obtain a valid IP address from a network administrator or your ISP. If your network does not need to access the Internet directly (or if address translation software mediates Internet access on your behalf), you can assign "private IP" addresses from a number of reserved address ranges that the InterNIC has set aside for this purpose. To learn more about these private address ranges and how to use them, you can download a copy of RFC 1918 from the InterNIC at *ftp://ds.internet.net/rfc/rfc1918.txt*. (As an alternative, you can read a hypertext version of this document at *http://www.cis.ohio-state.edu/rfc/rfc1918.txt*.)

If you select Specify an IP address, the remaining three boxes become active. When you're finished, the IP Address box should display the correct IP address for that computer.

If you're entering an IP address into an entry box, press the period key to jump from one octet to the next. This comes in handy when an address does not contain a three-digit number in any octet field. You can also use the right arrow key to advance the insertion point, but don't use the Tab key—it advances the insertion point to the next input field and forces you to backtrack to complete the IP address specification.

As described earlier, the subnet mask defines which part of the IP address represents the network and which part represents the host. You must supply this information or your computer will not be able to communicate using TCP/IP.

The default gateway for a computer defines the host, usually a router, to which the computer should send data that is not destined for the computer's subnet. For example, if a computer's address is 156.24.99.10 with a subnet mask of 255.255.255.0, its host address is 10 and its network address is 156.24.99. If this computer had data to send to a computer whose address was 203.15.13.69, it would send the packets to the default gateway for forwarding to the appropriate network. Whenever connectivity to other networks is required, you must provide an IP address for the default gateway on the machine's network segment. If you don't, traffic from your machine will not be able to get to machines that aren't on the same network segment as your computer.

Pressing the Advanced button opens the window shown in Figure 7-7. The IP addresses area allows you to assign multiple addresses to one network adapter, whereas the Default gateways area provides support for multiple router configurations.

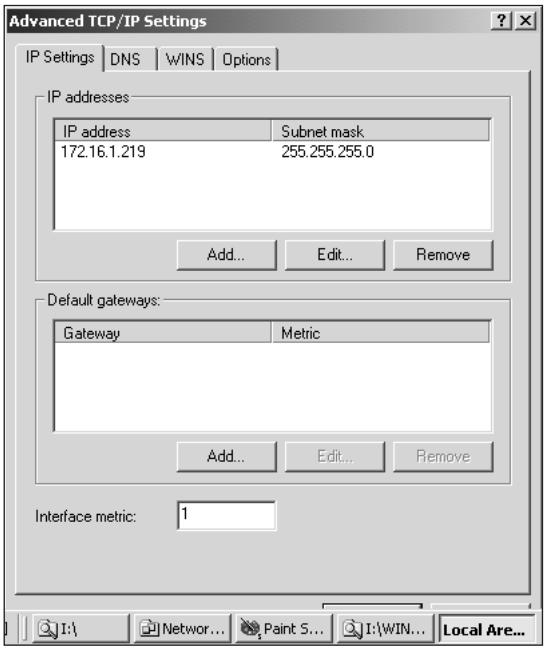

Figure 7-7 The Advanced TCP/IP Settings dialog box, IP Settings tab

By selecting the DNS tab, shown in Figure 7-8, the user is able to configure DNS on his or her computer. Multiple DNS servers can be defined along with setting their use priority. You can also define how incomplete domain names or host names are resolved (for example, by adding suffixes to create a fully qualified domain name).

Use the WINS tab (see Figure 7-9) to configure WINS settings. You can define multiple WINS servers and set their use priority. You can also enable or disable the use of an LMHOSTS file. Furthermore, you can enable, disable, or save the setting to the DHCP server whether or not this system will use NetBIOS over TCP/IP.

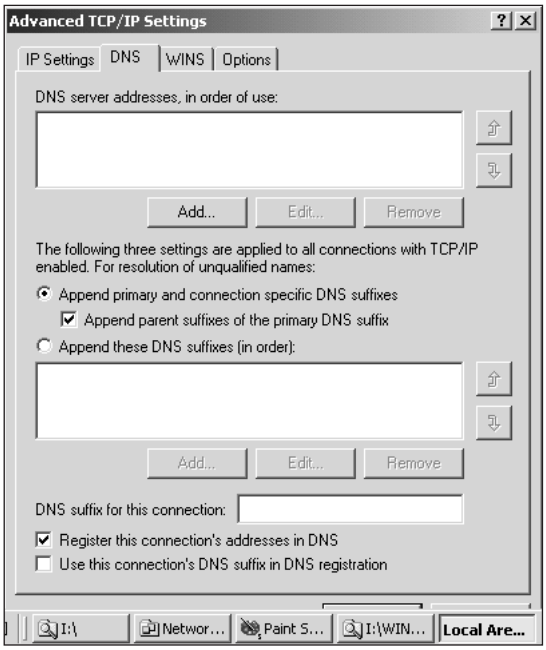

Figure 7-8 The Advanced TCP/IP Settings dialog box, DNS tab

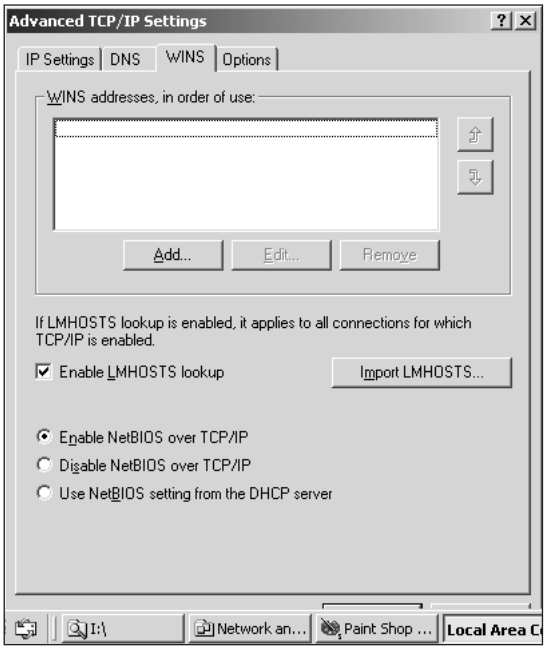

Figure 7-9 The Advanced TCP/IP Settings dialog box, WINS tab

The Options tab lists optional TCP/IP-related services or capabilities. The two default optional items are IP Security and TCP/IP filtering. Selecting a listed item and clicking Properties reveals a service-specific configuration dialog box. For more information about configuring these and other optional items, consult the *Windows 2000 Resource Kit*.

CHAPTER SUMMARY

- Windows 2000 supports three core network transport protocols: NetBEUI, NWLink (IPX/SPX), and TCP/IP. Each of these protocols works best on a network of a particular size, where each such network has its own special performance and access requirements.
- Windows 2000 Professional provides network access primarily by using TCP/IP. TCP/IP is routable, supports enterprise-level networks, and has been designed to interconnect dissimilar types of computers, which helps to explain why it's the protocol of choice on the Internet. TCP/IP is an industry-standard protocol that provides easy cross-platform communication.
- Interprocess communication (IPC) defines communication among the Windows 2000 operating system's threads and tasks. IPC also applies to networked computers; it defines a way for client computers to request services from some servers and permits servers to reply to requests for services. In Windows 2000, IPC mechanisms fall into two categories: programming interfaces and file systems.
- Windows 2000 includes a number of applications that utilize TCP/IP and provide Internet connectivity. In spite of TCP/IP's complexity, configuring Windows 2000 to employ this protocol is not difficult.

KEY TERMS

Address Resolution Protocol (ARP) — The IP protocol used to resolve numeric IP addresses into their MAC layer physical address equivalents.

Asynchronous Transfer Mode (ATM) — A cell-oriented, fiber- and copper-based networking technology that supports data rates from 25 Mbps to as high as 2.4 Gbps.

binding — The process of developing a stack by linking network services and protocols. The binding facility allows users to define exactly how network services operate in order to optimize the network performance.

boundary layer — Microsoft term for an interface that separates two classes of network or other system components. Boundary layers make it simpler for developers to build general-purpose applications without requiring them to manage all the details involved in network communications.

Client Service for NetWare (CSNW) — Service included with Windows 2000 Professional that provides easy connection to NetWare servers.

connectionless — A class of network transport protocols that makes only a "best effort" attempt at delivery, and that includes no explicit mechanisms to guarantee delivery or

data integrity. Because such protocols need not be particularly reliable, they are often much faster and require less overhead than connection-oriented protocols.

connection-oriented — A class of network transport protocols that includes guaranteed delivery, explicit acknowledgment of data receipt, and a variety of data integrity checks to ensure reliable transmission and reception of data across a network. Although reliable, connection-oriented protocols can be slow because of the overhead and extra communication.

Data Link Control (DLC) — A network transport protocol that allows connectivity to mainframes, printers, and servers running Remote Program Load software.

Domain Name Service (DNS) — TCP/IP service that is used to resolve FQDN names to IP addresses.

Dynamic Data Exchange (DDE) — A method of interprocess communication within the Windows operating system.

Dynamic Host Configuration Protocol (DHCP) — An IP-based address management service that permits clients to obtain IP addresses from a DHCP server. This allows network administrators to control and manage IP addresses centrally, rather than on a per-machine basis.

Ethernet II — An older version of Ethernet that preceded the 802.3 specification, offering the same 10 Mbps as standard Ethernet, but using a different frame format.

Fiber Distributed Data Interface (FDDI) — A 100 Mbps fiber-based networking technology.

File Transfer Protocol (FTP) — The protocol and service that provides TCP/IP-based file transfer to and from remote hosts and confers the ability to navigate and operate within remote file systems.

HOSTS — A static file placed on members of a network to provide name resolution between hosts and IP addresses.

Internet Control Message Protocol (ICMP) — The protocol in the TCP/IP suite that handles communication between devices about network traffic, quality of service, and requests for specific acknowledgments (such as those used in the PING utility).

Internet Protocol (IP) — The protocol that handles routing and addressing information for the TCP/IP protocol suite. IP provides a simple connectionless transmission that relies on higher-layer protocols to establish reliability.

Internetwork Packet Exchange (IPX) — The protocol developed by Novell for its NetWare product. IPX is a routable, connectionless protocol similar to IP but much easier to manage, and with lower communication overhead.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) — The two primary protocols developed by Novell for its NetWare network operating system. IPX/SPX is derived from the XNS protocol stack and leans heavily on XNS architecture and functionality. See also IPX and SPX.

interprocess communication (IPC) — The mechanism that defines a way for internal Windows processes to exchange information.

LMHOSTS — File used in Microsoft networks to provide NetBIOS name-to-address resolution.

Multiple Universal Naming Convention Provider (MUP) — A Windows 2000 software component that allows two or more UNC providers (for example, Microsoft networks and NetWare networks) to exist simultaneously. The MUP determines which UNC provider will handle a particular UNC request and forwards the request to that provider.

Multi-Provider Router (MPR) — A file system service that can designate the proper redirector to handle a resource request that does not use UNC naming. The MPR lets applications written to older Microsoft specifications behave as if they used UNC naming. The MPR is able to recognize those UNCs that correspond to defined drive mappings.

NetBIOS Enhanced User Interface (NetBEUI) — A simple transport program developed to support NetBIOS installations. NetBEUI is not routable, so it is not appropriate for larger networks.

Network Basic Input/Output System (NetBIOS) — A client/server interprocess communication service developed by IBM in 1985. NetBIOS presents a relatively primitive mechanism for communication in client/server applications, but allows an easy implementation across various Microsoft Windows computers.

Network Driver Interface Specification (NDIS) — Microsoft specification that defines parameters for loading more than one protocol on a network adapter.

Network Dynamic Data Exchange (NetDDE) — An interprocess communication mechanism developed by Microsoft to support the distribution of DDE applications over a network.

Network File System (NFS) — A UDP-based networked file system originally developed by Sun Microsystems and widely used on many TCP/IP networks. (Windows 2000 does not include built-in NFS support, but numerous third-party options are available.)

NWLink — Microsoft's implementation of Novell's IPX/SPX protocol suite.

Open Datalink Interface (ODI) — A part of the Novell protocol suite that provides the ability to bind more than one protocol to an adapter.

Packet Internet Groper (PING) — An IP-based utility that can be used to check network connectivity or to verify whether a specific host elsewhere on the network can be reached.

redirector — Software that examines all requests for system resources and decides whether such requests are local or remote.

remote execution (rexec) — The IP-based utility that permits a user on one machine to execute a program on another machine elsewhere on the network.

remote shell (rsh) — The IP-based utility that permits a user on one machine to enter a shell command on another machine on the network.

Reverse Address Resolution Protocol (RARP) — Used to map from a MAC-layer address to a numeric IP address.

Sequenced Packet Exchange (SPX) — A connection-oriented protocol used in the NetWare environment when guaranteed delivery is required.

Server service — The Windows 2000 component that handles the creation and management of shared resources and performs security checks against requests for such

resources, including directories and printers. The Server service allows a Windows 2000 computer to act as a server on a client/server network, up to the maximum number of licensed clients.

Simple Mail Transfer Protocol (SMTP) — The IP-based messaging protocol and service that supports most Internet e-mail.

Simple Network Management Protocol (SNMP) — The IP-based network management protocol and service that makes it possible for management applications to poll network devices and permits devices to report on error or alert conditions to such applications.

subnet — A portion of a network that might or might not be a physically separate network. A subnet shares a network address with other parts of the network but is distinguished by a subnet number.

subnet mask — The number used to define which part of a computer's IP address denotes the host and which part denotes the network.

Telnet — The TCP/IP-based terminal emulation protocol used on IP-based networks to permit clients on one machine to attach to and operate on another machine on the network as if the other machines were terminals locally attached to a remote host.

Transmission Control Protocol/Internet Protocol (TCP/IP) — A suite of Internet protocols upon which the global Internet is based. TCP/IP is the default protocol for Windows 2000.

Transmission Control Protocol (TCP) — The reliable, connection-oriented, IP-based transport protocol that supports many of the most important IP services, including HTTP, SMTP, and FTP.

Transport Driver Interface (TDI) — The specification to which all Windows transport protocols must be written to be used by higher-layer services, such as programming interfaces, file systems, and interprocess communication mechanisms.

Trivial File Transfer Protocol (TFTP) — A lightweight alternative to FTP that uses UDP to provide only simple get-and-put capabilities for file transfer on IP-based networks.

Universal Naming Convention (UNC) — A multivendor, multiplatform convention for identifying shared resources on a network.

User Datagram Protocol (UDP) — A lightweight, connectionless transport protocol used as an alternative to TCP in IP-based environments to supply faster, lower overhead access, primarily (but not exclusively) to local resources.

Windows Internet Naming Service (WINS) — A service that provides NetBIOS name-to-IP-address resolution.

Workstation service — The Windows component that supports client access to network resources and handles functions such as logging on, connecting to network shares (directories and printers), and creating links using the Windows 2000 IPC options.

X.25 — An ITU standard for packet-switched networking; common outside of the United States where its robust handling makes it a good match for substandard telephone networks.

Review Questions

1. The _____ enables a system to determine which part of an IP address represents the host, and which part represents the network.
2. _____ is a TCP/IP service used to resolve host or domain names to addresses.
3. The _____ service can be used to automatically assign IP configurations to a computer.
4. The _____ file provides NetBIOS name-to-IP-address resolution.
5. _____ is a TCP/IP protocol that is used for file manipulation.
6. By changing the _____, you alter the order in which services are accessed.
7. _____ is the Microsoft service that provides NetBIOS name-to-IP-address resolution.
8. The _____ examines requests for system resources and decides whether they are local or remote.
9. NDIS allows any number of adapters to be bound to any number of transport protocols. True or False?
10. Of the following protocols, which is the fastest and best suited for small single-segment LANs?
    a. TCP/IP
    b. NWLink
    c. NetBEUI
    d. DLC
11. DLC supports which two of the following network functions? (Choose all correct answers.)
    a. direct connection to IBM mainframes
    b. terminal emulation services
    c. network routing
    d. access to network-attached printers
12. What Windows 2000 networking component allows a system to access shared resources?
    a. TCP/IP
    b. Workstation service
    c. RPC
    d. NetDDE

13. If you are assigned the IP address 172.16.1.1, what full class subnet mask is most likely the correct one to use?
    a. 255.0.0.0
    b. 255.255.0.0
    c. 255.255.255.0
14. What class of IP addresses offers the most flexibility with regard to subnetting by providing for the most number of hosts?
    a. Class A
    b. Class B
    c. Class C
15. What should be placed on remote systems that connect to routed networks over slow WAN links? (Choose all correct answers.)
    a. NetBEUI
    b. LMHOSTS
    c. DNS
    d. HOSTS
    e. WinInet
16. What TCP/IP command can test the presence of a remote system?
    a. Telnet
    b. PING
    c. ARP
    d. Route
17. Which of the following is the static text-based equivalent of the Windows 2000 NetBIOS name-to-IP-address resolution service?
    a. HOSTS
    b. LMHOSTS
    c. DNS
    d. WINS
18. If your network hosts the correct service, you do not need to configure TCP/IP to participate in a network. True or False?
19. Which of the following protocols is used to inquire if an address is reachable on the Internet?
    a. SMTP
    b. UTP
    c. PING
    d. IMAP

20. What two IPC interfaces are used by Windows 2000 for file system access? (Choose all correct answers.)
    a. WinSock
    b. named pipes
    c. mailslots
    d. OLE
21. Which protocols can be used on a network where the clients are granted Internet access? (Choose all correct answers.)
    a. NetBEUI
    b. NWLink
    c. TCP/IP
22. The NetBEUI protocol under Windows 2000 can support a maximum of _____ devices on a network.
    a. 16
    b. 64
    c. 254
    d. 1023
23. What is provided by NDIS and ODI?
    a. Dynamic client configuration
    b. Distribution of driver software
    c. Binding of multiple protocols to multiple adapters
    d. Resolution of names to IP addresses
24. Which of the following will reduce broadcasts the most in a TCP/IP environment?
    a. DNS
    b. WINS
    c. NWLink
    d. DLC
25. TCP/IP is the most widely used protocol in the world. True or False?

HANDS-ON PROJECTS

Project 7-1

To view the status and properties of a Local Area Connection:

This project assumes that your Windows 2000 Professional system is connected to a network.

1. Open the Network and Dial-up Connections dialog box (click **Start**, select **Settings**, and then click **Network and Dial-up Connections**).
2. Select the **Local Area Connection** object.
3. From the **File** menu, select **Status**.
4. This reveals the Status dialog box. Notice the details provided on this dialog box: connection status, duration, speed, and packets.
5. Click the **Properties** button.
6. This reveals the Properties dialog box for this connection. Notice how this dialog box reveals the NIC involved with this connection and all of the services and protocols associated with this connection.
7. Click **Cancel** to close the Properties dialog box.
8. Click **Close** to close the Status dialog box.
9. Close the Network and Dial-up Communications dialog box.

Project 7-2

To use PING to test TCP/IP communications:

This project assumes that you are connected to a TCP/IP network. You must know the IP address or host name or domain name of at least one system on your network (or the Internet if you also have Internet access).

1. Open the Command Prompt by clicking on the **Start** menu, then selecting **Programs**, then selecting **Accessories**, then clicking **Command Prompt**.
2. Type **PING <*IP address or name*>** where <*IP address or name*> is the IP address of a system on your network, the name of a system on your network, or the domain name of a system on the Internet. Press **Enter**.
3. You should see a statement similar to "Pinging 172.16.1.7 with 32 bytes of data:" followed by four lines listing whether a reply was received or a timeout occurred.
4. Close the Command Prompt by typing **exit** and then pressing **Enter**.

Project 7-3

To view the HOSTS and LMHOSTS sample files:

1. Open Notepad by clicking on the **Start** menu, then selecting **Programs**, then selecting **Accessories**, and then clicking **Notepad**.
2. From the File menu, select **Open**.
3. Use the Open dialog box to locate and select the **\Winnt\System32\drivers\etc** directory. This can be accomplished by using the Up One Level button to move to a parent container or by double-clicking on a displayed drive or folder to move to a child container.
4. Change the Files of type to **All Files** by using the pull-down list.
5. You should see a list of files in this folder. Select **hosts**, then click **Open**.
6. Scroll down through this file, reading the information it provides. Do not make any changes to the file at this time.
7. From the File menu, select **Open**. You should still be viewing the \etc directory.
8. Change the Files of type to **All Files** by using the pull-down list.
9. You should see a list of files in this folder. Select **Lmhosts.sam**, then click **Open**.
10. Scroll down through this file, reading the information it provides. Do not make any changes to the file at this time.
11. From the File menu, select **Exit**.

Project 7-4

To configure TCP/IP:

The IP address of 172.16.1.1 and subnet mask of 255.255.255.0 can be replaced by your own assigned values.

1. Open the Network and Dial-up Connections interface. Click **Start**, select **Settings**, then click **Network and Dial-up Connections**.
2. Select the **Local Area Connection** object.
3. Click the **File** menu, then click **Properties**. This reveals the Properties dialog box for the selected Local Area Connection object.
4. Select the **Internet Protocol (TCP/IP)** in the list of components.
5. Click **Properties**. This reveals the Internet Protocol (TCP/IP) Properties dialog box.
6. Select the **Use the following IP address** radio button.
7. Type the IP address of **172.16.1.1**.
8. Type in the subnet mask of **255.255.255.0**.

9. Click **OK**.
10. Click **OK**.
11. Click the **File** menu, then click **Close**.
12. Restart the system for the changes to take effect.

Project 7-5

To view network bindings:

1. Open the Network and Dial-up Connections interface. Click **Start**, select **Settings**, then click **Network and Dial-up Connections**.
2. Click the **Advanced** menu, then click **Advanced Settings**. This reveals the Advanced Settings dialog box where bindings are managed.
3. Select a connection from the connection box.
4. Notice the contents of the lower field, where installed services and protocols are listed in their binding order.
5. Notice that the items closer to the top of the list are bound in priority to those listed lower on the list.
6. Notice the check box beside each item that allows you to disable that service or protocol.
7. Click **Cancel** to ensure you've made no changes.
8. Click the **File** menu, then click **Close**.

Project 7-6

To install and remove NetBEUI:

1. Open the **Network and Dial-up Connections** interface. Click **Start**, select **Settings**, then click **Network and Dial-up Connections**.
2. Select the **Local Area Connection** object.
3. Click the **File** menu, then click **Properties**. This reveals the Properties dialog box for the selected Local Area Connection object.
4. Click the **Install** button.
5. Select **Protocol** from the list of Network Component Types.
6. Click **Add**.
7. Select **NetBEUI Protocol** from the list of Protocols.
8. Click **OK**.
9. Notice that NetBEUI now appears in the list of network components.
10. Select **NetBEUI Protocol**.
11. Click **Uninstall**.
12. Click **Yes** when asked to confirm the deletion.

13. If prompted to reboot, click **Yes**.
14. Close the Properties dialog box.
15. If not prompted to reboot, click the **File** menu, then click **Close**. Then reboot the system by clicking the **Start** menu and then clicking **Shutdown**. Select **Restart**, then click **OK**.

CASE PROJECTS

1. Describe the functions and features of TCP/IP included with Windows 2000.
2. As a network administrator at XYZ Corp., you always hear about it when performance problems arise on the network. In the past two weeks, you've been involved in switching the network over from using NetBEUI exclusively, to a mixture of NetBEUI and TCP/IP. You've installed TCP/IP on all Windows 2000 Server and Professional systems, and made sure that all the machines are properly configured. Because the network is growing, and an additional cable segment has been added, with more planned for the future, you plan to switch entirely from NetBEUI to TCP/IP over time. All of a sudden, your users complain that the network has slowed dramatically. What steps can you take that might improve speed performance? Which machines should you make changes on, and why?